

Allarmi & Avvisi

(i tutorial di Alessandro de Simone)

Copyright Alessandro de Simone 2007 (www.alessandrodesimone.net) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore (www.alessandrodesimone.net) per gli accordi del caso.

Copyright Alessandro de Simone 2007 (www.alessandrodesimone.net) - No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document - even if partially - without author's written authorization. Websites and publishing house who wish to employ this document must write the author (www.alessandrodesimone.net).

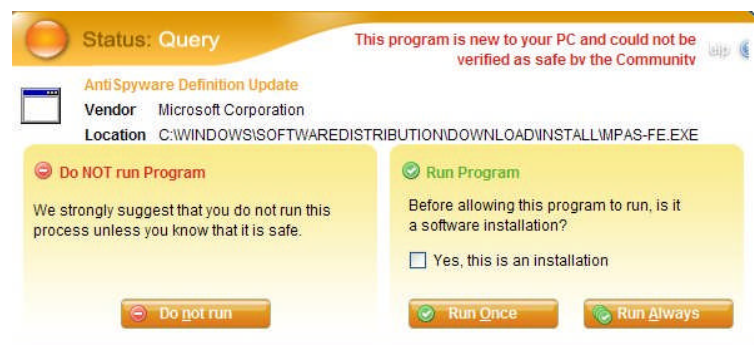
Niente panico

Che cosa bisogna fare quando sul video compaiono allarmanti messaggi?

Come rispondere a domande il cui significato è poco chiaro? In questo tutorial descrivo ciò che mi è successo nel corso di una normale connessione a Internet. Ovvio che si tratta di un caso specifico e abbastanza particolare, ma può essere utile per acquisire esperienza.

Non appena stabilii la connessione a Internet comparve la finestra di avviso riportata qui in alto, generata dal programma stabilmente attivo in background *Windows Worms Doors Cleaner* (che descriverò in un prossimo Tutorial) che in realtà dovrebbe limitarsi a sovrintendere al controllo delle porte. Ciò significa, quindi, che le funzioni di questo

programma svolgono controlli più ampi di quanto si possa immaginare. Alla finestra di *Windows Worms Doors Cleaner* si aggiunse subito dopo quella di *PrevX* (anche questo programma verrà descritto in uno specifico tutorial) che evidenziava il tentativo di apertura da parte di un programma - MPAS-FE.EXE - di cui ovviamente non sapevo assolutamente nulla. La cosa che mi allarmò maggiormente era la collocazione di questo nuovo e sconosciuto programma: si trattava infatti della cartella riservata a Windows, e in particolare alla installazione di programmi scaricati dal web. La memorizzazione di un programma sconosciuto, per giunta in una cartella così particolare, non deve essere presa alla leggera, anche se - come vedremo - si trattava di un programma originale Microsoft,



utile (anzi, indispensabile) per scaricare patch e aggiornamenti. La prudenza mi impose di negare l'apertura del programma e la comparsa della rassicurante finestra di PrevX, che ne confermava il blocco, mi permise di sospendere temporaneamente l'attività per visitare

un sito un po' particolare. Si trattava del prezioso...

www.what-process.com

...che descrive l'origine e l'utilizzo di un'enorme quantità di file – EXE e DLL soprattutto – più o meno noti. Nella schermata, riprodotta integralmente qui a destra, apprendo che il file incriminato – **mpas-fe.exe** – era in realtà un componente di *Windows Defender*, creato da Microsoft e utilizzato negli aggiornamenti automatici. Il fatto che *Windows Worms Doors Cleaner* ne segnalasse la presenza, derivava unicamente dal tentativo di alterazione di una zona di memoria, abitualmente "stabile". Per quanto riguardava gli avvisi di PrevX, poi, non c'era motivo di allarmarsi perché il programma avvisa costantemente ogni tentativo di esecuzione di un programma per lui sconosciuto.

Aggiornamenti periodici

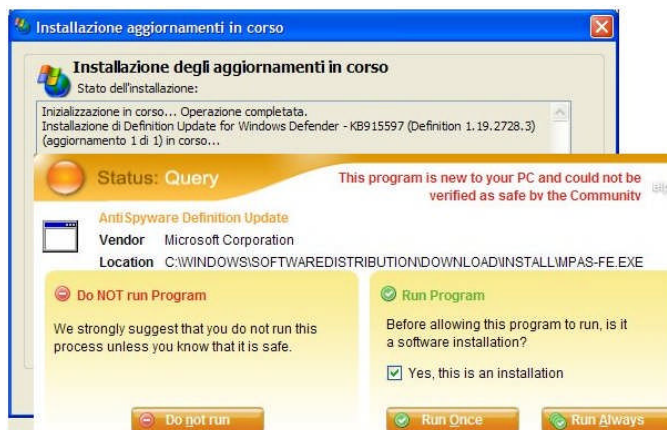
Chiarito un dubbio, se ne presentava subito un altro: come è noto, Microsoft raggruppa patch e aggiornamenti – rendendoli disponibili a tutti – solo il primo martedì di ogni mese. L'esperienza di cui mi occupo in queste pagine si riferiva invece all'ultima settimana del mese. Per accertarsi che non vi fosse alcunché di anomalo decisi quindi di "forzare" l'aggiornamento a *Windows Update*, cliccando sul noto pulsante *Start/Windows Update*. La schermata riprodotta qui a destra confermava che era effettivamente disponibile un nuovo aggiornamento originale Microsoft, che provvidi subito a scaricare. *PrevX*, il programma "guardiano" del mio PC che operava costantemente in background,

The screenshot shows a web browser window displaying the 'What Process?' website. The page title is 'mpas-fe.exe - Process Info - What Is mpas-fe.exe?'. The main content area is titled 'What Process Home > Process Library > mpas-fe.exe'. A red circle highlights the text 'User Comments On mpas-fe.exe'. Below this, there are two user comments. The first comment, posted by 'Mark' on 4/30/2006, states: 'This process was named by ZoneAlarm as wanting to change the registry to cause "wextract-cleanupo" to run each time the computer was started - seems to be related to W32 Cabinet Self-Extractor'. The second comment, posted by 'Michel' on 8/14/2006, states: 'This is a component of Microsoft Windows Defender. Microsoft Defender, formerly Windows Anti-spyware, is an anti-spyware application that scans the user PCs for various types of malware, and runs a variety of other security features.' Below the comments is a 'Post A Comment About mpas-fe.exe' form with fields for 'Enter Message*', 'Name*', 'Email Address', and 'IP Address: Logged'. The page also features a sidebar with links like 'Search Google', 'Search MSN', and 'Get WinTasks Pro'. At the bottom, there is a disclaimer: 'Disclaimer: Uretopia makes no claims as to the accuracy of information on this website. Please contact us should contributions to the site be offensive. Uretopia Limited offers "What Process?" software download free of any charge. It can be distributed freely. By downloading and using the software, you agree to do so at your own risk and that Uretopia Limited will not be held liable for any problems that occur as a result.'

The screenshot shows the Microsoft Windows Update website. The page title is 'Microsoft Windows Update'. The main content area is titled 'Windows Update' and features a search bar and navigation links. The primary section is 'Risultati analisi rapida' (Quick analysis results), which includes a 'Verifica e installa aggiornamenti' (Check and install updates) button. Below this, there is a section for 'Aggiornamenti a priorità alta' (Priority updates), which lists a 'Microsoft Windows Defender' update: 'Definition Update for Windows Defender - KB915597 (Definition 1.19.2728.3)'. The update details include 'Dimensioni download: 0 KB, 0 minuti' and 'Scaricato e pronto per l'installazione'. The page footer contains the Microsoft logo and copyright information: '©2007 Microsoft Corporation. Tutti i diritti sono riservati. Note legali | Marchi | Informativa sulla privacy'.

continuava ovviamente a non fidarsi del nuovo intruso (*mpas-fe.exe*) che tentava nuovamente di installarsi.

La procedura di download veniva quindi immediatamente messa in pausa (vedi figura qui a destra, sullo sfondo) dimostrando che la difesa in atto sul PC era perfettamente attiva. Dopo aver consentito a *PrevX* di considerare il programma come una nuova installazione autorizzata, la procedura di download e di installazione procedeva correttamente e si concludeva in pochi secondi.



Conclusioni

Quando compaiono finestre di avviso non è mai prudente trascurarle. Sul web vi sono molti strumenti validi per verificare situazioni particolari, e magari venirne a capo. La prudente abitudine di scaricare aggiornamenti deve riferirsi non solo al programma antivirus usato abitualmente, ma anche (soprattutto?) al sito Microsoft, costantemente attenta ai problemi relativi alla sicurezza. La comparsa di finestre di avviso, nel corso dei periodici aggiornamenti, verifica indirettamente l'attività dei programmi preposti alla difesa del nostro PC che operano in background.

Verifica la disponibilità di eventuali aggiornamenti di questo Tutorial, o la pubblicazione di altre documentazioni, visitando periodicamente il sito:

www.alessandrodesimone.net

Altri siti con i quali collaboro:

easyHDR PRO 1.30 - <http://www.easyhdr.com> - Programma grafico per la gestione della modalità HDR

FastSum: <http://www.fastsum.com> Programma per la creazione dell'impronta digitale dei file (metodo MD5)

TagTuner: <http://www.tagtuner.com> Programma per la gestione dei file musicali

**Il presente Tutorial è stato modificato il giorno 30 giugno 2007
Per ulteriori aggiornamenti consultare il sito www.alessandrodesimone.net**